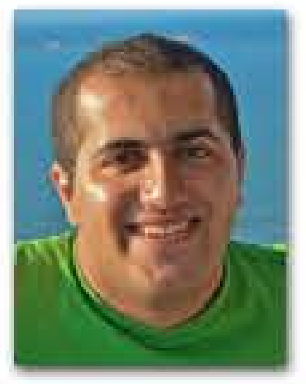
Design of Action and Alliance Strategy in Defense against Anonymous Cyber Threats

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University



MIT Political Science Department
Supervisor: Dr. Nazli Choucri
Mina Rady

Cyber Security & the Governance Gap:
Complexity, Contention, Cooperation
MIT, January 6th and 7th, 2014

This work is funded by the Office of Naval Research under award number N00014-09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s)and do not necessarily reflect the views of the Office of Naval Research.

ABSTRACT:

Anonymity, a major feature of the cyberspace, is a common channel to a multitude of threats. Despite efforts to defend against anonymous threats, their rapid evolution challenges the sustainability of any designed strategy for cyber defense. A sustainable cyber defense strategy must be able to dynamically adapt to information about new threats and to utilize international alliance when necessary without violating fundamental ethics. Our earlier research in 2012 analyzed ways to influence anonymous networks that can either undermine the network performance or undermine the anonymity of connecting users. Earlier we concluded that most influential control actions are accessible to State level actors. Here we propose a defense strategy design approach that begins with assessment of the control capacities of State actors over the given threat space (in our case, anonymity). Then we delineate the various motivations for States to exercise control over anonymous communication. We suggest a strategy design process that rests on alliance with States who share the control motivation and who possess highest possible control capacity. This strategy relies on a quality-controlled information system based on mapping new information about the Cyberspace into a compatible hierarchical classification.

1) Scopes of Action

We differentiate between two scopes of control actions that are feasible to a state: explicit or implicit.

The explicit scope of action is public: pursuit of actions in this scope requires direct and public intervention of the state.

The implicit scope of action is low profile: an action in this scope can technically be done on the individual level and therefore, individuals representing the state can exercise this action without necessarily expressing publicly the state identity.

State level control actions

Explicit

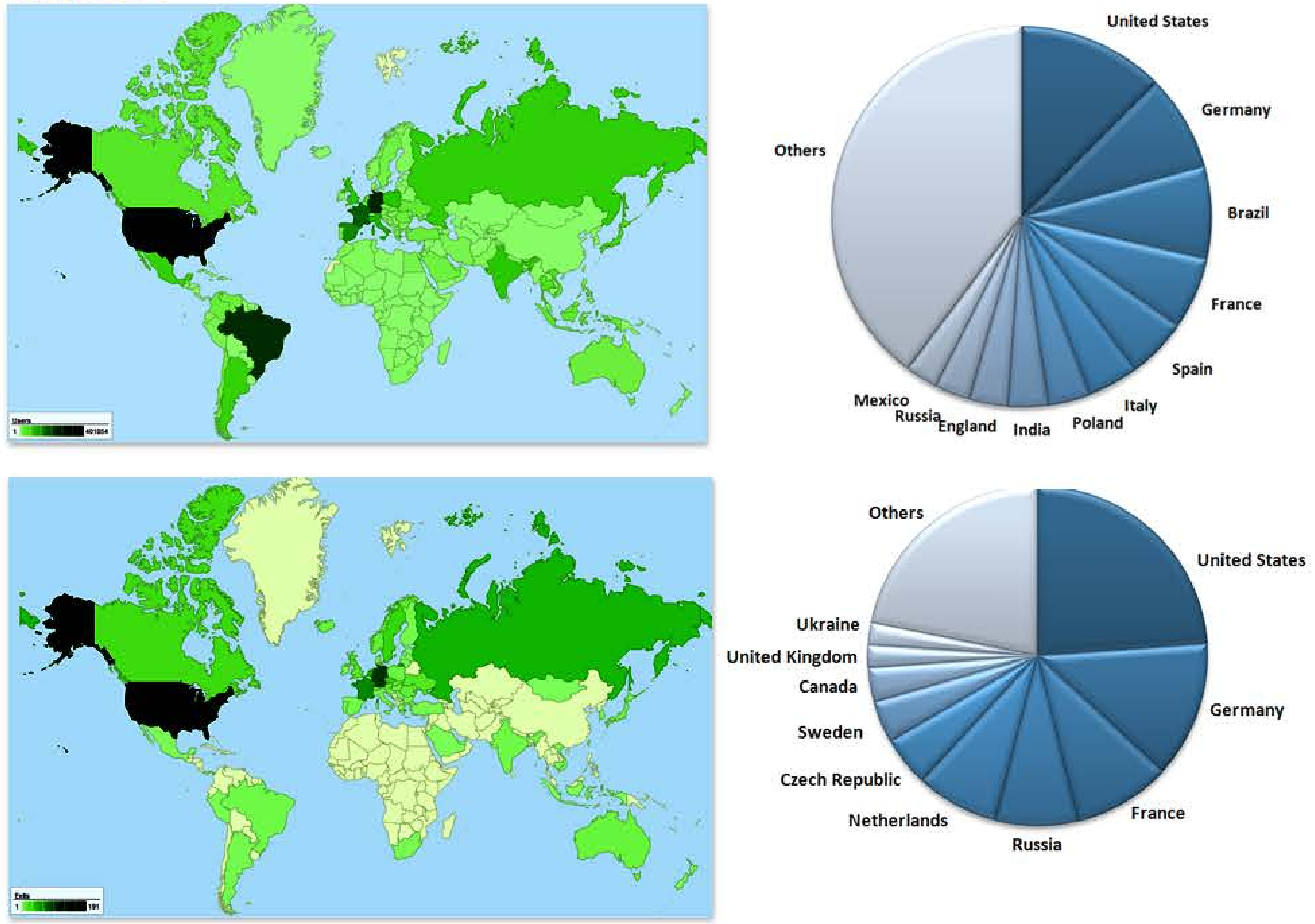
- Web Site/ mirror blockage
- Public relay blockage
- IX level traffic analysis
- Deep Packet Inspection
  - To distinguish and block traffic with Tor fingerprint
  - To distinguish and block SSL traffic.

Implicit

- Disseminate infliterated copies of Tor software (through social forums).
- Deploy infliterated entry/exit nodes that monitor communication.
- Embed tracking code to be executed on client machine in server response

Most explicit control actions are with higher influence if the state includes higher number of Tor proxies in its jurisdiction. The influence is also higher if the percentage of Exit proxies is higher since control actions on exit proxies affect whole Tor routing path regardless how many countries routing path extends. In addition, the more Tor users the country includes, the higher the traffic the country generates on the network which affects the network performance and anonymity.

The following visualizations are for the global political distribution of 1) Tor users and 2) Tor exit proxies



2) Motivations of State Level Action

State level control motivations

Internal

- Local counter terrorism efforts
- Domestic political conflict
- Domestic social norms

External

- Threats imposed by anonymous international organized crime/terrorism
- Human rights violations by the anonymous global child abuse content network.
- Online black markets for drugs, forged identities, cyber mercenaries etc.
- Global Cyber Attacks

Examples:

- CHINA: Political and social censorship.
- IRAN: establishment of governance upper hand in a conflict between the Iranian Government and the Iranian People.
- EGYPT:
  - -Partial blockage of the Internet in Sinai, in several occasions, to constraint Jihadist terrorist communication after Morsi's ouster.
  - -Full blockage of the Internet on January 26th 2011 in reaction to the mass protests.
- VARIOUS ARAB COUNTRIES: social censorship (expulsion of any means of access to pornographic content).
- SYRIA (possible): Internal conflicts between the government and Islamist opposition army.

3) Strategy Design

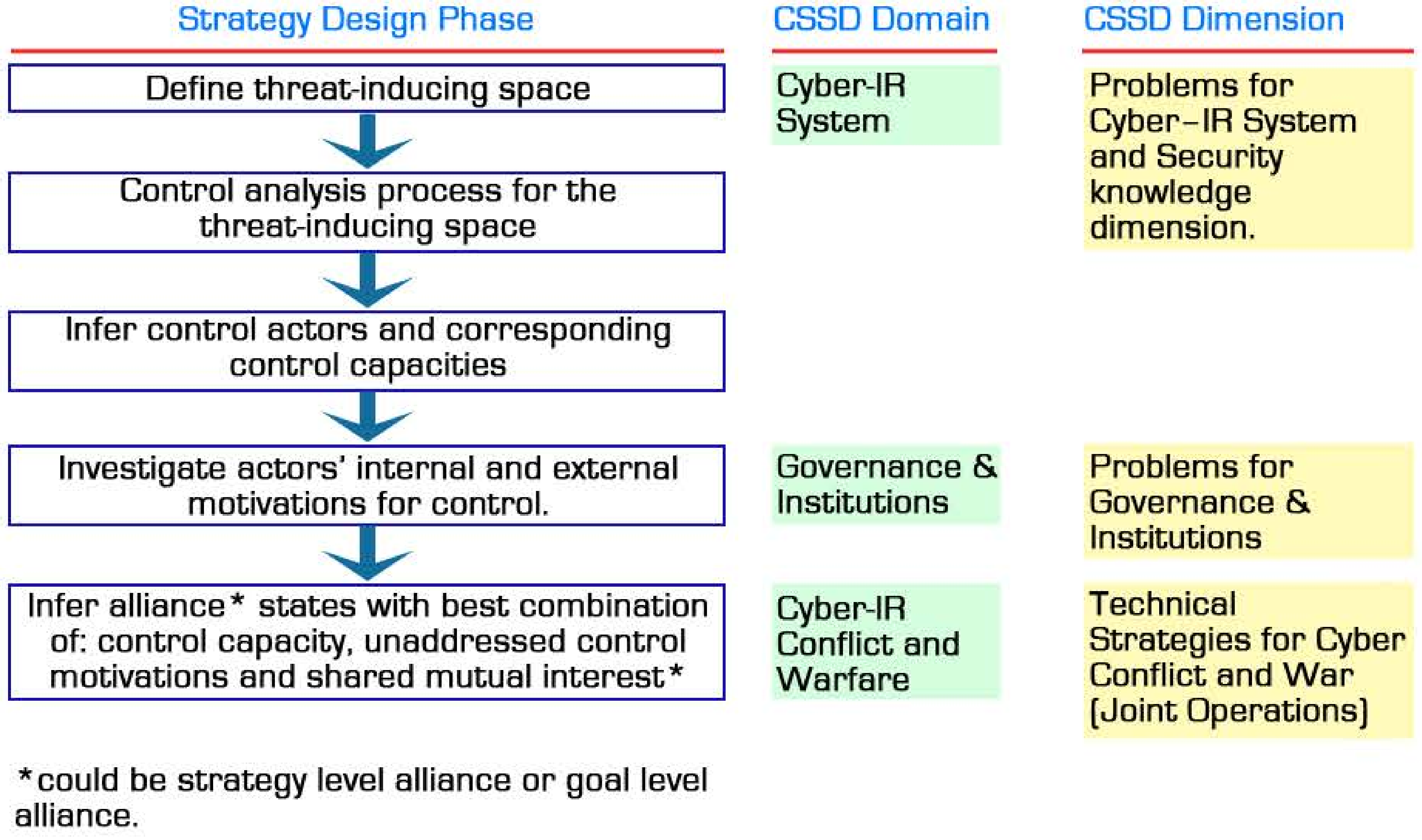
PHILOSOPHY

Most external state concerns are unmet concerns due to the state's lack of control on foreign actors. However, most external threats are shared and mutual threats (such as global illegal black markets, child abuse networks, global cyber attacks etc.). Therefore, there is an unused defense privilege available when states with mutual exposure to external threats ally. This alters the scope of the threats from being external to each country to being internal to the allied jurisdictions. Not only does that offer higher chances for neutralizing external threats, but it also increases the legitimacy of control actions taken by the alliance since control is being exercised according to "common norms". This increases the sustainability of the defense strategy on the long term from both operational and ethical points of views.

INFORMATION & DECISION SUPPORT

We propose to utilize an information system that provides decision support for our proposed strategy design process using information classification hierarchy that is compatible with our logic.

CSSD presents knowledge about Cyberspace according to defined dimensions and domains. To construct each phase of our strategy design process, supporting information would be classified under corresponding intersection of domains and dimensions. The following is our mapping between each design phase and corresponding location of relevant information in CSSD.



Strategy Design Phase	CSSD Domain	CSSD Dimension
Define threat-inducing space	Cyber-IR System	Problems for Cyber–IR System and Security knowledge dimension.
Control analysis process for the threat-inducing space		
Infer control actors and corresponding control capacities		
Investigate actors' internal and external motivations for control.	Governance & Institutions	Problems for Governance & Institutions
Infer alliance* states with best combination of: control capacity, unaddressed control motivations and shared mutual interest*	Cyber-IR Conflict and Warfare	Technical Strategies for Cyber Conflict and War (Joint Operations)

*could be strategy level alliance or goal level alliance.